The Limitations of Technical Mechanisms as Proxies for Context

Position paper - work in progress

Catherine Dwyer

Seidenberg School of Computer Science & Information Systems, Pace University, New York, NY
cdwyer@pace.edu

ABSTRACT

Contextual Integrity (CI) argues that information flow should be governed by context dependent norms. But representing context within technical systems is challenging, and information will flow whether or not context has been adequately established. If software developers cannot determine context, they may turn to technically based mechanisms as a substitute. One technical mechanism used to reason about information flow is the origin of the data itself, whether it is volunteered, observed, or inferred. Volunteered data is shared directly by the user, observed data records user activity, and inferred data is calculated via algorithmic analysis. This paper will explore the use of volunteered, observed, and inferred categories as a proxy for context, describing problematic privacy outcomes. A plan to investigate the scope of this issue within technical systems will be presented, along with suggestions for mechanisms to mitigate this condition.

CCS CONCEPTS

• **Security and privacy ~ Human and societal aspects of security and privacy** • Privacy protections

KEYWORDS

Contextual Integrity, privacy by design, information flow.

1 Introduction

A critical element in the adoption of CI within technical systems is operationalization of context. The challenge of representing context faithfully within technical systems has been explored in "Contextual Integrity Through the Lens of Computer Science," [1] an in-depth literature review of CI within computer science research. CI theory conceives of context as relating to a specific social sphere, for example a school or a health setting. Instead, computer science research depends on situations, rather than social spheres, as a stand in for context. Computer science research "conceptualizes contexts as concrete and at least partly technical … We note that as far as CI is concerned, it is essential that contexts be understood as normative, as one important trait of contexts is that they have ends, purposes, and values" [1].

Technical context can influence expectations regarding the flow of information. Whether an app is active is factored when considering requests for data such as location. There is a kind of reasoning that goes on as to whether the app 'needs' data for a specific task that informs information flow [1].

In technical systems such as online social networks (OSNs), contexts are overlapping and evolutionary. Computational models of CI "assume the existence of well-defined contexts, in which individuals enact pre-defined roles and information sharing is governed by an explicit set of norms," [2]. OSNs, on the other hand have difficulty with information leaking from one context to another.

1.1 CI Decision Heuristic

CI based research that considers the role of context applies the CI decision heuristic, a methodology developed to address "when and why some of these [privacy] alterations provoke legitimate anxiety, protest, and resistance," [3]. The decision heuristic includes these steps: 1) Describe the new practice in terms of information flows. 2) Identify the prevailing context and identify potential impacts from contexts nested in it. 3) Identify information subjects, senders, recipients. 4) Identify transmission principles. 5) Locate applicable entrenched informational norms and identify significant points of departure. 6) Prima facie

assessment - A breach of information norms yields a prima facie judgment that contextual integrity has been violated because presumption favors the entrenched practice. 7) Evaluation I: Consider moral and political factors affected by the practice in question. 8) Evaluation II: Ask how the system or practices directly impinge on values, goals, and ends of the context. 9) On the basis of these findings, contextual integrity recommends in favor of or against systems or practices under study [3].

Research using the CI decision heuristic include an analysis of personal blogs [4], cloud technology: [5], social network sites [6], the Internet of Things [7]. An application of the CI decision heuristic to location data [8] echoed concerns regarding the processing of location data based on technical considerations rather than normative ones. The article refers to "three types of data with a large impact on autonomy, identity, and privacy: volunteered, observed, and inferred data," [8]. These categories identify the technical methods that enable the capture of personal data, and are particularly salient to policy discussions on personal liberties [9, 10]. The next section will define these categories and discuss the relevance of these categories to CI.

1.2 Volunteered, Observed, and Inferred Data

This section will describe the differences between volunteered, observed, and inferred data. Volunteered data is data that is freely given by the user. This can be a picture shared on Facebook, or billing information needed for a financial transaction. Volunteered data is typically collected with explicit consent, that is, there is a defined dialogue of interactions where the user is asked and agrees to allow the capture of data. The request for consent does not need be a simultaneous with the capture of data. For example, when you join Facebook you give consent to share photos, but you are not asked again for consent every time you share a photo. Instead your consent is "remembered," that is stored as a property associated with that information flow.

The next category is observed data, it consists of digital data generated by the activities of a user, for example browsing history, phone location data, and other digital records of activity captured through technology. This category can be obtained without the explicit, real time consent of the user. For example, when you go to a website, the browser you are using shares information about the device you are using, along with access to stored cookies. Observed data has more value if it can be associated with a specific "user" tagged with an anonymous identifier, or personally identified through items such as email address or cell phone number. Observed data can include IP addresses, time spent on a specific site, and the step by step history going from one site to another. Observed data also includes related cookies. Cookie data may contain unique identifiers that can be used to connect new activity with previous records of online activity.

Next is inferred data, which is the product of an algorithm or other automated process that combines volunteered and observed data, and associates patterns of activity with a particular trait or quality of interest. Examples include credit scores, and predictions regarding purchase intention. Inferred data are calculated values often expressed as a probability value, for example 90% likely or 12% unlikely. The delivery of personalized content, behavioral targeting, and other individualized treatments are built from inferred data [11].

Algorithmic predictions grow more reliable as more data is added and integrated into the existing profile or archive. This becomes an incentive to collect whatever data is available, since it may be of use for a calculated result in the future. Another factor that reinforces the collection of as much data as possible is the low cost of data storage. The cost of digital storage has dropped significantly in the last 20 years. Because large data sets (i.e. Big Data) are inexpensive to maintain, and accrue value over time, there is an economic incentive to keep them continually updated.

2 Problem Statement

The CI decision heuristic begins by decomposing the subject of interest into a series of information flows. As shown in [1] and [8], decisions regarding information flow can be influenced by technical contexts. If software developers cannot determine an acceptable context, they investigate the origin of the information. If the data has been volunteered, the developer will assume user consent. If it is observed, an assumption can

be made that consent is not needed (i.e. no expectation of privacy in public). If it is inferred, then the assumption is it has been anonymized.
These assumptions need to be considered through the lens of CI. How can information flows be analyzed if they are determined by these three distinctions? How can technical platforms operationalize privacy protections around the status of information as volunteered, observed, or inferred? The first step in answering these questions is to examine cases where information flow has been determined based on the categories of volunteered, observed, and inferred data. The next sections will discuss two examples, one involving location data, and the second involving data shared through OSNs.

2.1 Location Data and Smart Phones

Location is represented computationally as two floating point numbers, one that represents latitude, and one for longitude. In most technical systems, floating points numbers take up 8 bytes of storage [12], or 16 bytes in total for both latitude and longitude. Since smart phones come with gigabytes of memory, the storage and transmission demands for location information are minuscule. In some ways, location is the perfect type of data when considering cost versus benefit. Location uses the bare minimum of computing resources, and results in significant added value when made available to advertisers [13].
In order to demonstrate how location data can be volunteered, observed, or inferred, we will use two fictional users, Alice and Bob. The volunteered scenario is straightforward. Alice wants to share her location with Bob, so she explicitly requests than an app such as Google Maps transmit her location data to Bob's smart phone.
An example of observed location data is possible with any app that has been given permission to access location data. This permission setting is set when the app is installed, and can be turned on or off by the user through privacy settings. If an app is active on Alice's phone and has permission to access location data, then that app may share location data with a third party mobile advertising company such as AdMob in order to sell location based advertising. In most cases involving advertising, the location is associated with a pseudo-anonymous identifier rather than Alice's explicit identity.
An example of location that is inferred takes advantage of information resources that map the locations of wireless access points. A crowd sourced map of wireless access points can be found at wigle.net (https://wigle.net/) . Similar maps are maintained by Google and Apple. As Alice travels around with her smart phone, it picks up nearby wireless signals. Even if Alice's phone does not connect, there is a communication protocol between Alice's phone and wireless access points. An app can use the Google Geolocation API to estimate location by passing the identity of at least two nearby wireless access points along with their relative signal strength [14]. Note that Alice's location can be calculated even if she has all location permissions turned off, as long as the wireless services on her phone are enabled.

2.2 Analysis of OSN Data

A valuable data asset associated with OSNs is the members' list of friends. This next case will look at how Facebook's friends list was exploited by the political consulting firm Cambridge Analytica to direct targeted advertising for the 2016 US presidential campaign [15].
Data was first collected using a Facebook app called "This Is Your Digital Life." The app was a personality quiz. When Facebook members installed this app, they agreed to share their Facebook data with the app, including their list of Facebook friends, as required by the terms of service for Facebook[1]. The app used the list of friends to build a dataset each friend's public Facebook data, including name, hometown, and any public "likes." Of particular interest were "likes," because they can used to infer personality traits [16].
To document the information flow from the Cambridge Analytica episode we will once again call upon our fictional users, Alice and Bob. It begins when Alice and Bob join Facebook and connect, i.e. become friends. Bob volunteers to Facebook that he is friends with Alice, and vice versa.

[1] Before 2017 this was required, it has since been removed as a requirement by Facebook.

Alice is an active Facebook user, and supports her favorite TV show "Duck Dynasty" by "liking" its page. Alice volunteers this to Facebook. Bob "likes" the page for the Fox TV show "Empire." Bob volunteers this to Facebook, and the default setting for "likes" is public, meaning there are no restrictions on access.
Alice signs up for the app "This Is Your Digital Life." As part of its terms of service, Alice agrees (volunteers) to share her list of Facebook friends, including Bob. Through this connection with Alice, the app "This Is Your Digital Life" accesses (observes) Bob's public information, including his name, home town, and public "likes." The Facebook data of Alice and Bob is turned into personality profiles that Cambridge Analytica uses to target political advertising to them. Alice is predicted (inferred) as a likely Trump voter, based in part on her "like" of Duck Dynasty [17]. By "liking" Empire, Bob is profiled as a resident of the "the Black Belt … a swath that [includes] city centers and other places with large nonwhite populations," [17]. Bob is predicted (inferred) to be a likely Clinton voter, and receives political advertising designed to diminish enthusiasm for the Clinton candidacy [18].

3 Discussion

As shown in these two cases, a series of information flows can disclose sensitive information such as a person's location or political orientation. Each incremental step in the information flow can be explained by its status as volunteered, observed, or inferred. But when the analysis of information flow focuses on the little steps that lead to sensitive data, there is no clear place to fix the flow. An app running on a smart phone has access to the identity of nearby wireless access points, that seems reasonable. Facebook "likes" are publicly available. So instead of ethical norms informing information flow, the assumptions tied to the categories of volunteered, observed, and inferred then inform technology design decisions.

4 Next Steps

The use of volunteered, observed, and inferred data as a proxy for context can lead to poor privacy outcomes. In order to explore how this works in practice, the next step will be to develop an app for the Google Android OS that determines location using all three methods: volunteered, observed and inferred. Once this app is operational, subjects will be recruited to use the app and record their reactions as their location is derived from different mechanisms.
There certainly are bad actors within the privacy space, but the intent of this research is to give software developers the benefit of the doubt, and expect they will act in good faith to identify the prevailing context and build appropriate information flows. But software developers cannot do the right thing if the tools they need are not be available. The issues identified in this position paper circle around to the critical role of values in design [19]. Because technical systems are the embodied architecture for public goods such as education, health care, and civic engagement, they need to have ends, purposes, and values built in that reinforce rather than weaken social structures. It is certainly a challenging task, but there are still some Roman aqueducts that continue to be in use. Once something is built that works the right way, it can stay around for a long time.

REFERENCES

[1] Benthall, S., Gürses, S. and Nissenbaum, H. *Contextual integrity through the lens of computer science*. Now Publishers Incorporated, 2017.
[2] Criado, N. and Such, J. M. Implicit contextual integrity in online social networks. *Information Sciences*, 325 (2015), 48-69.
[3] Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.
[4] Grodzinsky, F. and Tavani, H. T. Applying the "Contextual Integrity" Model of Privacy to Personal Blogs in the Blogoshere. Computer Science & Information Technology Faculty Publications, 2010,
[5] Grodzinsky, F. and Tavani, H. T. Privacy in 'The Cloud': Applying Nissenbaum's Theory of Contextual Integrity. In *Proceedings of the ACM SIGCAS Computers and Society* (2011).
[6] Sar, R. K. and Al-Saggaf, Y. Contextual integrity's decision heuristic and the tracking by social network sites. *Ethics Inf Technol*, 16 (2014), 15-26.

[7] Winter, J. S. Surveillance in ubiquitous network societies: normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. *Ethics and Information Technology*, 16, 1 (2014), 27-41.
[8] Hildebrandt, M. Location Data, Purpose Binding and Contextual Integrity: What's the Message? in *Protection of Information and the Right to Privacy-A New Equilibrium?*, edited by L. Floridi, Springer, Switzerland, 2014.
[9] WEF. *Personal data: The emergence of a new asset class*. World Economic Forum, 2011.
[10] WEF. *Rethinking personal data: Strengthening Trust*. World Economic Forum, 2012.
[11] Rubinstein, I. S. Voter privacy in the age of big data. *Wisconsin Law Review* (2014).
[12] IEEE *IEEE Standard for Floating Point Arithmetic*. IEEE, 2008.
[13] N.A. Location Based Service Market 2019 Leading Growth Drivers, Emerging Audience, Segments, Sales, Profits, Analysis, Size, Statistics. Reuters.com, February 18, 2019, https://www.reuters.com/brandfeatures/venture-capital/article?id=83809.
[14] Google Geolocation API Developer Guide. 2019, https://developers.google.com/maps/documentation/geolocation/intro.
[15] Cadwalladr, C. and Graham-Harrison, E. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, *The Guardian*, 03-17, 2018.
[16] Kosinski, M., Stillwell, D. and Graepel, T. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, 110, 15 (2013), 5802.
[17] Katz, J. 'Duck Dynasty' vs. 'Modern Family': 50 Maps of the U.S. Cultural Divide, *The New York Times*, December 27, 2016.
[18] Graham, D. A. Trump's 'Voter Suppression Operation' Targets Black Voters, *The Atlantic*, October 27, 2016.
[19] Nissenbaum, H. How computer systems embody values. *IEEE Computer*, 34, 3 (2001), 119-120.